PLIEGO DE PRESCRIPCIONES TÉCNICAS

CONTRATO DE SUMINISTRO MEDIANTE PROCEDIMIENTO ABIERTO

Expediente: 01-2024 CORTAFUEGOS PARA PROTECCIÓN DE LA RED DE DATOS CORPORATIVA
Poder adjudicador: BCBL- Basque Center on Cognition Brain and Language (BCBL)

1. OBJETO DEL SUMINISTRO

El objeto del presente procedimiento es contratar el suministro, instalación y puesta en funcionamiento de CORTAFUEGOS PARA PROTECCIÓN DE LA RED DE DATOS CORPORATIVA, cuyo uso se inscribe en el ámbito de la investigación básica en neurociencia cognitiva.

La importancia creciente de la ciberseguridad en el ámbito de las tecnologías de la información se acentúa en el caso de BCBL por la naturaleza de la información a proteger, que a menudo incluye datos personales de salud, registros de neuroimagen y grabaciones de voz y vídeo.

El suministro de un conjunto de cortafuegos de red compatible con el entorno descrito en el Anexo I, y capaz de asumir nuevas demandas, constituye un elemento crítico para la modernización de la infraestructura de tecnologías de la información del centro.

El contrato incluye la instalación, configuración y puesta en marcha de la solución, así como la garantía de la solución para un periodo de cinco años, contados a partir de que el proyecto de instalación se considere entregado.

Se entiende por garantía el mantenimiento sin cargo de todo el material, incluyendo:

- Cobertura 8x5xNBD mediante *partner*, con acceso a una línea de soporte en tiempo real.
- Acceso a recursos de documentación en línea facilitados por el fabricante de los equipos suministrados.
- Acceso a descarga de actualizaciones de software, así como parches y mejoras.
- Ninguno de los elementos hardware ofertados tendrá un horizonte previsible de discontinuidad, descatalogación o fin de vida a la hora de redactar la oferta.

Las entidades licitadoras deberán observar las siguientes condiciones generales:

- BCBL excluirá proyectos con características relevantes inferiores a las requeridas, o cuyo planteamiento se desvíe significativamente de la arquitectura de solución deseable.
- El licitador ha de ofertar soluciones que incluyan cuantos elementos hardware y software sean necesarios para garantizar la adecuada integración de los sistemas propuestos con el entorno de red existente.
- No se aceptarán propuestas que perjudiquen la continuidad de las políticas actuales de gestión IT.
- El licitador proporcionará formación al personal técnico designado por BCBL sobre configuración y operación de las nuevas soluciones, debiendo colaborar además en la redacción y/o adaptación de los procedimientos e instrucciones técnicas afectados.
- Con el objeto de garantizar el correcto funcionamiento de la solución, BCBL se reserva el derecho de solicitar al licitador baterías de pruebas del equipamiento ofertado. En tal caso BCBL se encargaría de especificar contenido y alcance de dichas baterías.
- Los equipos propuestos deberán integrarse en las ubicaciones físicas que BCBL designe a tal efecto, para lo cual el adjudicatario deberá encargarse del montaje de éstos en racks de anchura estándar, así como de su correcta interconexión a las redes de electricidad, almacenamiento y datos. Para ello el adjudicatario deberá proporcionar los elementos que se necesiten, como armarios, cables, regletas, adaptadores y alargaderas, así como las adaptaciones en los cuadros eléctricos si éstas fuesen necesarias. El etiquetado y la documentación sobre la instalación han de seguir las reglas que establezca

BCBL. Además, el adjudicatario se encargará de retirar todos los embalajes y restos de material de las instalaciones de BCBL, así como los equipos reemplazados.

- La planificación de los trabajos de implantación ha de cuidar el impacto sobre la operación normal del centro, considerando que la realización de ciertas tareas puede implicar la intervención de técnicos de la empresa adjudicataria fuera del horario laboral.

2. LUGAR DE ENTREGA DEL SUMINISTRO

El suministro de abastecimiento se realizará en la siguiente dirección: BCBL. Paseo Mikeletegi 69, 20009 Donostia-San Sebastián, Spain

Con carácter previo, el adjudicatario deberá enviar los requerimientos de instalación a BCBL al objeto de que puedan realizarse las adecuaciones necesarias.

3. CARACTERÍSTICAS BÁSICAS Y REQUERIMIENTOS TÉCNICOS

3.1. Requerimientos y características básicas de los equipos:

Conforme al escenario descrito en el Anexo I, el licitador suministrará equipamiento para sustituir las dos parejas de aparatos en los CPDs por una única agrupación de dos cortafuegos de nueva generación (en adelante, NGFW por sus siglas en inglés), en configuración Activo/Activo o Activo/Pasivo, con dominios virtuales diferenciados para filtrar tráfico perimetral e interno. Además, en cada una de los dos laboratorios mencionados en el Anexo I se instalarán un cortafuegos cuya única misión será la de establecer una conexión segura con los CPDs, descartando el resto del tráfico.

En la Tabla 1 se indican las características exigibles a cada uno de los tipos de cortafuegos. Como requisito imprescindible, los equipos ofertados deben figurar como cualificados en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del Centro Criptológico Nacional, documento CCN-STIC-105, edición Junio-2024.

TABLA 1: CARACTERÍSTICAS TÉCNICAS REQUERIDAS PARA PROVISIÓN DE CORTAFUEGOS

	Cortafuegos CPD	**Cortafuegos Laboratorio**
Funcionalidades		
VPN (IPSEC)	Sí	Sí
Inspección SSL (1)	Sí	-
Control de aplicación (2)	Si	-
Filtrado Web (3)	Sí	-
Prevención de ataques Día Cero (4)	Sí	-
Antivirus	Sí	-
Prevención de intrusiones (IPS)	Si	-
Filtrado DNS (5)	Si	-
Integración AD (6)	Sí	-
SD-WAN	Sí	-
Autenticación de doble factor (7)	Sí	-
Dominios virtuales	4	-
Rendimiento		
NGFW (8)	8 Gbps	-
Prevención de Amenazas (9)	4 Gbps	-
Hardware		
Interfaces 1GbE 10/100/1000 Base-T	8	4
Interfaces 1GbE SFP (10)	6	-
Interfaces 10GbE SFP+ (10)	4	-
Puerto dedicado alta disponibilidad	10 Gbps SFP+	-
Fuente alimentación redundante	Sí	-
Disco duro integrado	120GB	120GB

(1) Hace referencia a la posibilidad de descifrar y analizar tráfico TLS/SSL. Esta funcionalidad debe ser configurable por categoría de aplicación.
(2) Capacidad de identificar la aplicación que genera el tráfico, cualidad distintiva de los cortafuegos NGFW.
(3) Clasificación y bloqueo de sitios web con contenido malicioso o indeseable según políticas configurables.
(4) Característica que permite la detección de amenazas desconocidas, bien como resultado de algoritmos de predicción o basada en análisis en la nube en tiempo real.
(5) Detección y bloqueo de respuestas DNS sospechosas.
(6) Importación de usuarios de Directorio Activo con los fines de identificar tráfico, definir políticas y analizar registros de actividad en función de usuarios.
(7) Configuración de acceso a aplicaciones o servicios críticos mediante múltiples factores de autenticación.
(8) Rendimiento medido con filtrado en capa 7, incluyendo control de aplicación y registros de actividad (log), usando una combinación de aplicaciones.
(9) Rendimiento medido con las siguientes funcionalidades activadas: control de aplicación, sistema de prevención de intrusiones, la protección antivirus, prevención de ataques Día Cero, Filtrado DNS y registro de actividad (log), usando una combinación de aplicaciones.
(10) Incluidos transceptores del fabricante para fibra óptica tipo SR.

3.2. Servicios

- Transporte: Serán por cuenta del adjudicatario todos los gastos de transporte, seguro y otros, excepto los propios del acondicionamiento del local. Asimismo, el adjudicatario será responsable de la instalación del equipo, asegurando su plena operatividad una vez instalado.
- Plan de Instalación y puesta en funcionamiento: Descripción de todos los aspectos relativos a la efectiva instalación del equipo en la sede de BCBL, con todas las actuaciones que deberán realizarse, incluyendo su entrega, instalación, puesta en funcionamiento y migración completa de las configuraciones de los equipos reemplazados. El adjudicatario proporcionará los recursos necesarios (humanos y materiales) para la puesta en funcionamiento del equipo, de modo que quede en funcionamiento en condiciones normales de explotación, con todos los elementos instalados y configurados.
- Formación: El adjudicatario impartirá la formación necesaria que permita su uso dirigida al personal designado de BCBL. Estas acciones formativas se realizarán en las instalaciones de BCBL.

4. PLAZO DE ENTREGA

El plazo máximo para la entrega, instalación y puesta en marcha del equipo será de 10 semanas a contar desde la fecha de la firma del contrato.

Tras la fase de puesta en funcionamiento, y una vez validada la instalación por personal de BCBL, se entenderá que el equipo ha sido suministrado correctamente y se procederá a la firma de un acta de recepción por ambas Partes.

5. GARANTÍA Y SERVICIO DE MANTENIMIENTO

La garantía se extenderá a la totalidad del período anteriormente indicado de cinco años, considerado a partir de la firma del acta de recepción del equipo, una vez certificada y validada la instalación y su correcto funcionamiento.

El adjudicatario llevará a cabo el mantenimiento integral del equipo durante el periodo de garantía establecido anteriormente. El coste de la garantía queda incluido en el precio del suministro del equipo.

Esta garantía incluirá la reparación de cualquier avería o mal funcionamiento del equipo que pudiera producirse, con la finalidad de mantenerlo en perfecto estado de conservación y uso.

Si durante el plazo de garantía se acreditara la existencia cualquier tipo de desperfecto en cualquiera de los componentes que forman parte del equipamiento, BCBL tendría derecho a reclamar al adjudicatario la reposición de los bienes inadecuados o, si no fuera suficiente, la reparación o sustitución de los mismos.

6. SERVICIO TÉCNICO

El adjudicatario deberá contar con un servicio de apoyo y soporte técnico a disposición de BCBL, para consultas y solución de problemas. Este servicio deberá ser accesible y suficiente en cuanto a horarios, plazos de respuesta, capacidad técnica.

7. OBLIGACIONES DEL ADJUDICATARIO

El adjudicatario se compromete a tomar todas las medidas necesarias y a utilizar los medios humanos y materiales adecuados para suministrar de una manera óptima el equipo objeto de este contrato. Serán de su cargo todos los costes que origine este compromiso, especialmente los transportes del material contratado, del personal y de los medios auxiliares que sean necesarios para desarrollar su tarea.

Tras de la firma del contrato, la empresa adjudicataria tendrá la obligación de entregar e instalar el equipo de acuerdo con el plazo ofertado, y dejar el equipo en el punto de destino totalmente instalado y operativo.

La retirada del material de embalaje utilizado para proteger el equipo durante el transporte irá a cuenta del adjudicatario. No se entenderá instalado el equipo hasta que éste no se haya suministrado en su totalidad y retirado todo el material de embalaje.

Si durante el transporte, el montaje o la instalación el equipo sufriera algún tipo de daño, deterioro o perjuicio, deberá ser reparado o sustituido, tal como establezca BCBL y el adjudicatario no tendrá derecho a reclamar ninguna cantidad por este motivo.

La entrega e instalación del equipo será supervisada por personal del BCBL.

Durante el ejercicio de sus actividades, el adjudicatario será responsable de los desperfectos causados por sus trabajadores a personas y/o cosas en general, tanto si pertenecen al adjudicatario, como a BCBL o a terceros.

8. ORGANIZACIÓN Y EQUIPO DEL TRABAJO. CONDICIONES DEL SERVICIO.

La empresa adjudicataria deberá tener a su disposición el personal y contar con los medios materiales necesarios para el cumplimiento de las obligaciones del contrato objeto de licitación.

Por su parte, BCBL establecerá los medios de control que estime convenientes para constatar el total y correcto cumplimiento de la prestación por parte del adjudicatario.

El suministro será ejecutado con calidad, rigor y eficacia y con absoluto cumplimiento de todas las disposiciones legales, reglamentarias, normas y especificaciones en vigor que, de forma directa o indirecta, regulan la misma.

El personal que realice el suministro dependerá exclusivamente del adjudicatario y éste tendrá todos los derechos y deberes inherentes a su calidad de patrono y deberá cumplir bajo su exclusiva responsabilidad las disposiciones vigentes, o que se dicten en un futuro, en materia laboral, Seguridad Social, Seguridad y Salud y fiscal, quedando BCBL exento de cualquier responsabilidad que pudiera derivarse como consecuencia del incumplimiento por parte del adjudicatario de las obligaciones anteriormente indicadas.

Serán por cuenta del adjudicatario todos los gastos necesarios para el cumplimiento del contrato, así como las indemnizaciones que correspondan por los daños o perjuicios que puedan ocasionarse con motivo del cumplimiento del contrato.

Durante la vigencia del contrato, el adjudicatario queda obligado a presentar, previo requerimiento de BCBL, cuanta documentación se le solicite, al objeto de acreditar el cumplimiento de las obligaciones de este contrato.

9. ACTA DE RECEPCIÓN

Una vez el equipo esté instalado y puesto en funcionamiento e impartida la formación, se realizará la correspondiente acta de recepción.

Anexo I. Despliegue de cortafuegos en BCBL

BCBL dispone de dos centros de procesamiento de datos (CPD) ubicados en edificios separados en el Parque Tecnológico de Donostia-San Sebastián. Uno de ellos se encuentra en nuestras instalaciones de Paseo de Mikeletegi 69, y el otro en la sala de Terceros de IZFE (Empresa pública informática de la Diputación de Gipuzkoa). Ambos CPDs se comunican mediante una línea de fibra óptica dedicada cuyo trazado mide 2 kilómetros de longitud.

En el CPD principal, situado en Paseo Mikeletegi, disponemos de:

- Una pareja de cortafuegos Palo Alto 850 configurados en Activo/Pasivo,
- Red troncal a 25 Gbps.
- Dos salidas a Internet:
    - I2basque: caudal de 10 Gbps simétricos, con 127 direcciones IP asignadas.
    - Sarenet: caudal de 600 Mbps simétricos, con 31 direcciones IP asignadas.

Y en el CPD secundario, ubicado en la sala de Terceros de IZFE (Empresa pública informática de la Diputación de Gipuzkoa):

- Dos cortafuegos Palo Alto 220 en configuración Activo/Pasivo
- Salida a internet con presencia de 300 Mbps simétricos con 15 direcciones IP asignadas.
- Troncal de red local a 25Gbps.

Ambos CPD se interconectan mediante una conexión de 20Gbps sobre fibra oscura (DWDM 2x10Gbps). A través de ella extendemos las VLAN del CPD principal al de respaldo.

Publicamos diversos servicios (correo electrónico, páginas web, servicios de red, etc.) en las tres conexiones, aunque sólo aquéllos considerados esenciales tienen asignada IP en los tres rangos. Las dos parejas cortafuegos descritas actúan tanto de muro perimetral como interno (segmentación de red), en mucha mayor medida el del CPD principal que el del respaldo, ya que todas las puertas de enlace residen en los PA850 excepto una que está en la otra pareja.

La Tabla 2 describe la distribución de enlaces en los cortafuegos del CPD principal.

TABLA 2: INTERFACES EN CORTAFUEGOS PALO ALTO PA-850

Nombre	Tipo	VLAN	Descripción
Ethernet1/1	1Gbps BaseT	70, 241	Testeo, Gestión
Ethernet1/2	1Gbps BaseT	242,243,247,248	Laboratorios
Ethernet1/3	1Gbps BaseT	56,80,81	Clinica y ERP
Ethernet1/4	1Gbps BaseT	45,85,86	ThinClients
Ethernet1/5	1Gbps BaseT	11	ICX con FW IZFE
Ethernet1/6	1Gbps BaseT	48,244,248	WiFi
Ethernet1/7	1Gbps BaseT	245,246	Laboratorios
Ethernet1/8	1Gbps BaseT	HA	
Ethernet1/9	10Gbps SFP+	50,52	PC's usuarios, HPC
Ethernet1/10	10Gbps SFP+	210,211	ISP
Ethernet1/11	10Gbps SFP+	54,240	DDBB, DMZ
Ethernet1/12	10Gbps SFP+	51,53,55	Mobility, email

En el CPD de respaldo, la tabla de enlaces es notablemente más reducida, como se muestra en la Tabla 3.

TABLA 3: INTERFACES EN CORTAFUEGOS PALO ALTO PA-220

Nombre	Tipo	VLANs	Descripción
Ae1	Trunk 2 x 1Gbps BaseT	140	DMZ Izfe
Ae2	Trunk 2 x 1Gbps BaseT	10,11	ICX FW BCBL
Ae3	Trunk 1 x 1Gbps BaseT	76,77	NAC (no activo)

En la Tabla 4 se pueden consultar otros datos de interés para estimar la complejidad de las configuraciones a migrar de los cortafuegos existentes.

TABLA 4: OTROS DATOS DE INTERÉS

	CPD BCBL	CPD IZFE
Reglas NAT	169	43
Reglas Seguridad	320	65
Reglas de reenvío basado en políticas	17	5
Objetos de red	573	78

El número de sesiones y el tráfico de cada firewall puede ser consultado libremente en el siguiente panel de Grafana:

https://kontuz.bcbl.eu/user/d/c818332c-7580-460f-937b-a50a669a24ac/statistics-pa?orgId=2

Ademas de los CPD descritos, BCBL cuenta con laboratorios en dos sedes, conectados mediante enlaces FTTH de 300Mbps simétricos.

La Figura 1 representa la topología descrita. Sin embargo, la renovación del equipamiento solicitada según las características descritas en la Tabla 1 introduce tres novedades:

- Reemplazo de las dos agrupaciones de cortafuegos existentes por una única de 2 cortafuegos, uno en cada CPD, configurados en alta disponibilidad Activo/Pasivo o Activo/Activo según recomendación del licitador.
- Separación en dos instancias virtuales del tráfico perimetral y el tráfico interno, generando así una arquitectura de dos capas.
- Provisión de cortafuegos para los laboratorios. En este caso no se requerirán trabajos de instalación o migración.

La Figura 2 muestra el escenario propuesto como resultado de la implantación.

FIGURA 1: ESCENARIO ACTUAL

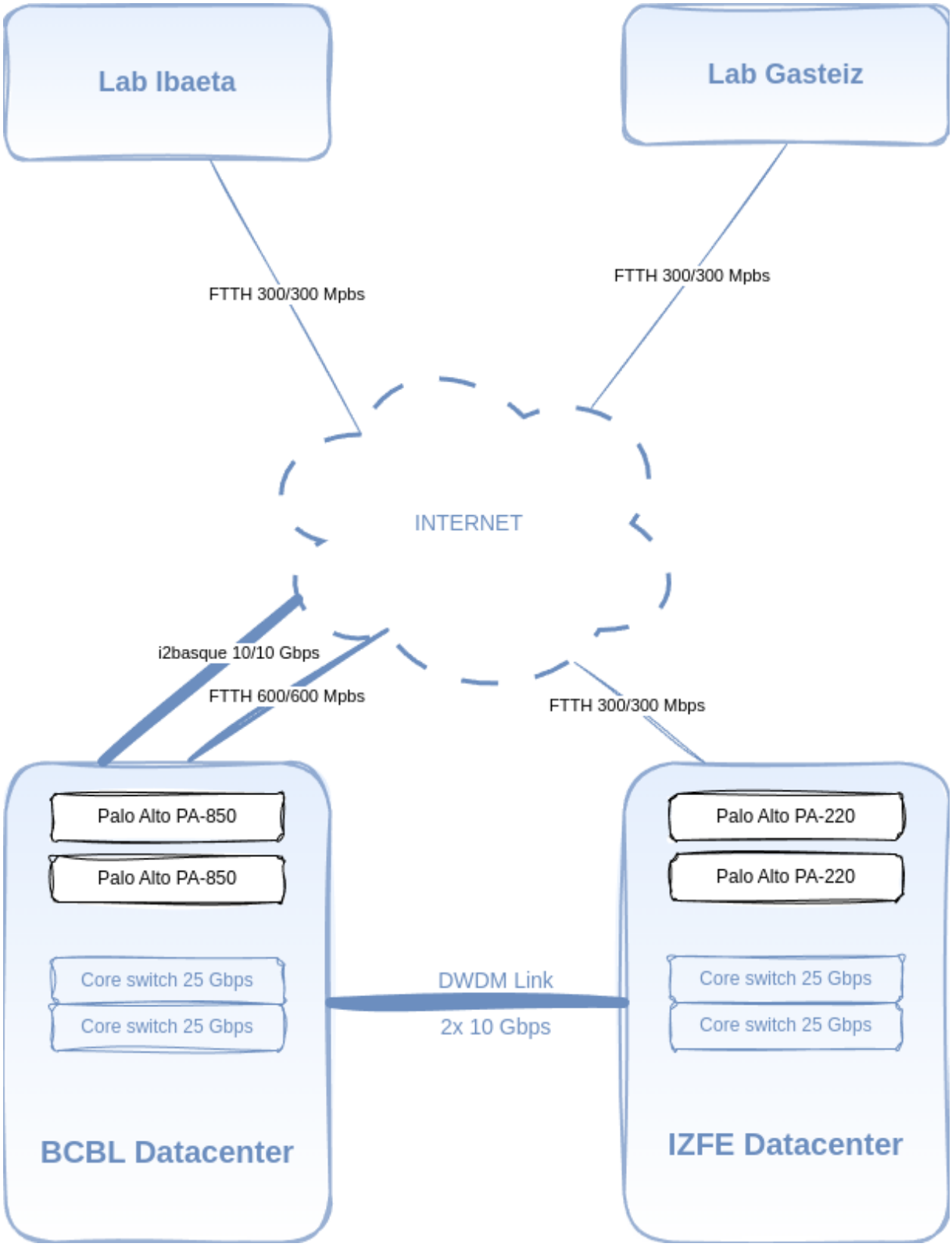


FIGURA 2: ESCENARIO PROPUESTO

